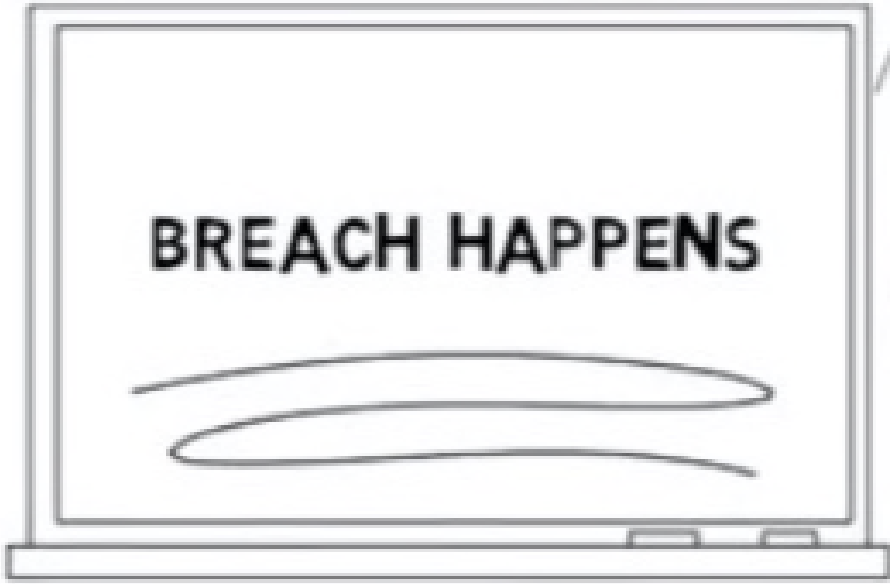

Morgan Lewis
TECHNOLOGY MAY-RATHON
Success in Cyber Incident Response in 2020
May 6, 2020
Gregory T. Parks
Ezra D. Church
Kristin M. Hadgis
© 2020 Morgan, Lewis & Bockius LLP

SECTION 01

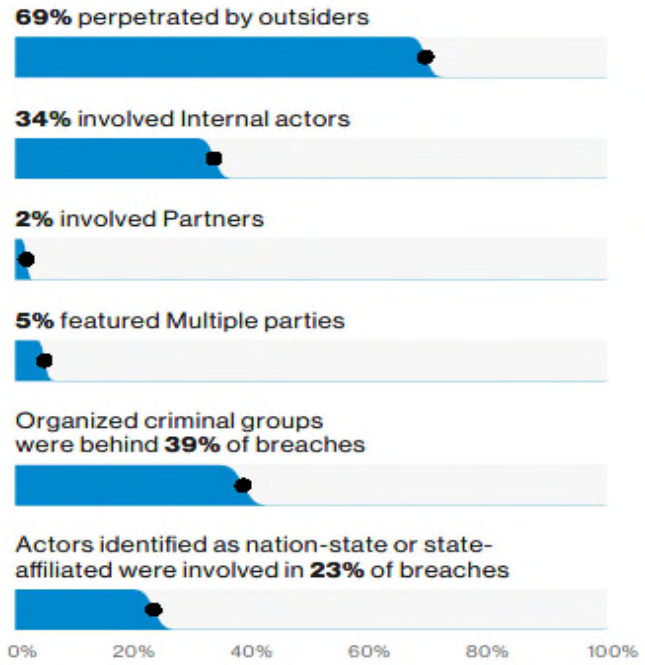
DATA BREACH BASICS

Data Breach Reality

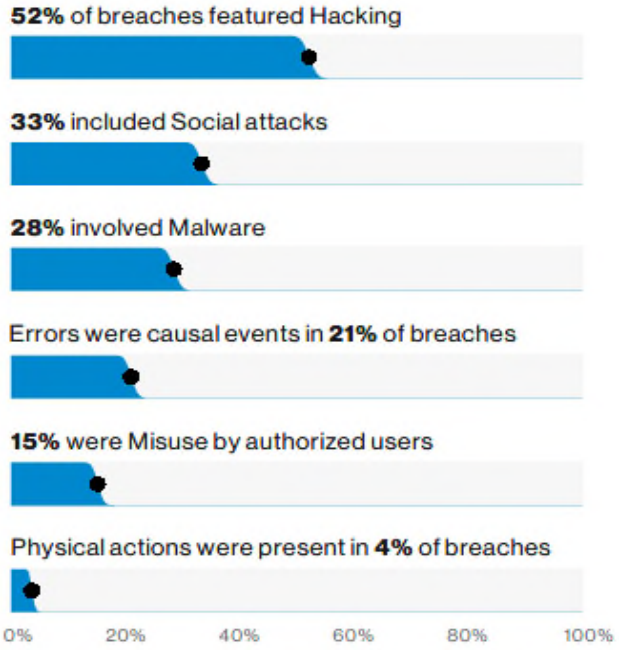


Data Breach – Who, What, Why, When, and How?

Who's behind the breaches?



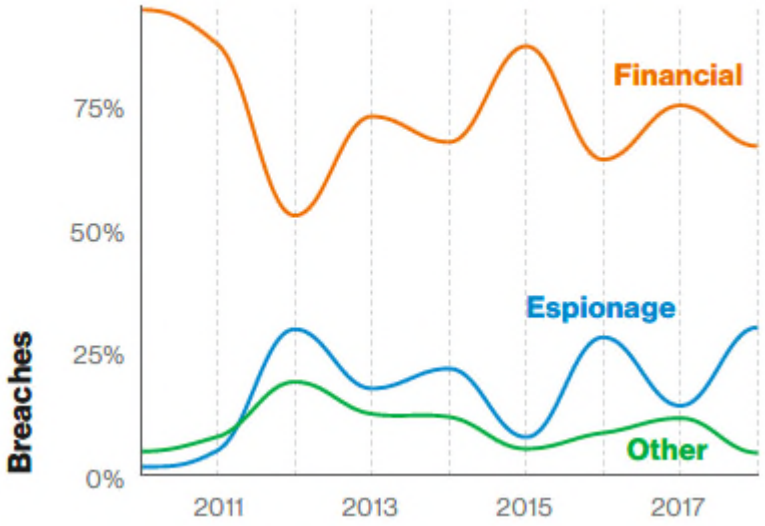
What tactics are utilized?



Source: Verizon Data Breach Investigations Report, 2019

Data Breach – Why?

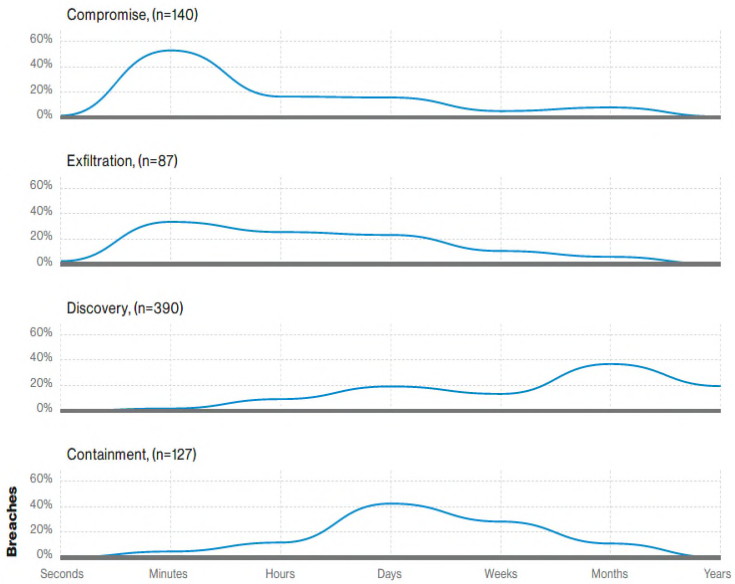
Actor motives in breaches



Source: Verizon Data Breach Investigations Report, 2019

Data Breach – When?

Breach timelines



Minutes to Compromise;
Hours to Exfiltrate;
Months to Discover;
Days to Contain

Hackers are getting better at covering their tracks

Source: Verizon Data Breach Investigations Report, 2019

Data Breach – How Much?

> Average total cost of a data breach:

$3.92 million

> Average cost per lost or stolen record:

$150

> Likelihood of a recurring material breach over the next two years:

29.6%

> Average total one-year cost increase:

1.5%

> One-year increase in cost per lost or stolen record:

1.3%

> Average cost savings with an Incident Response team:

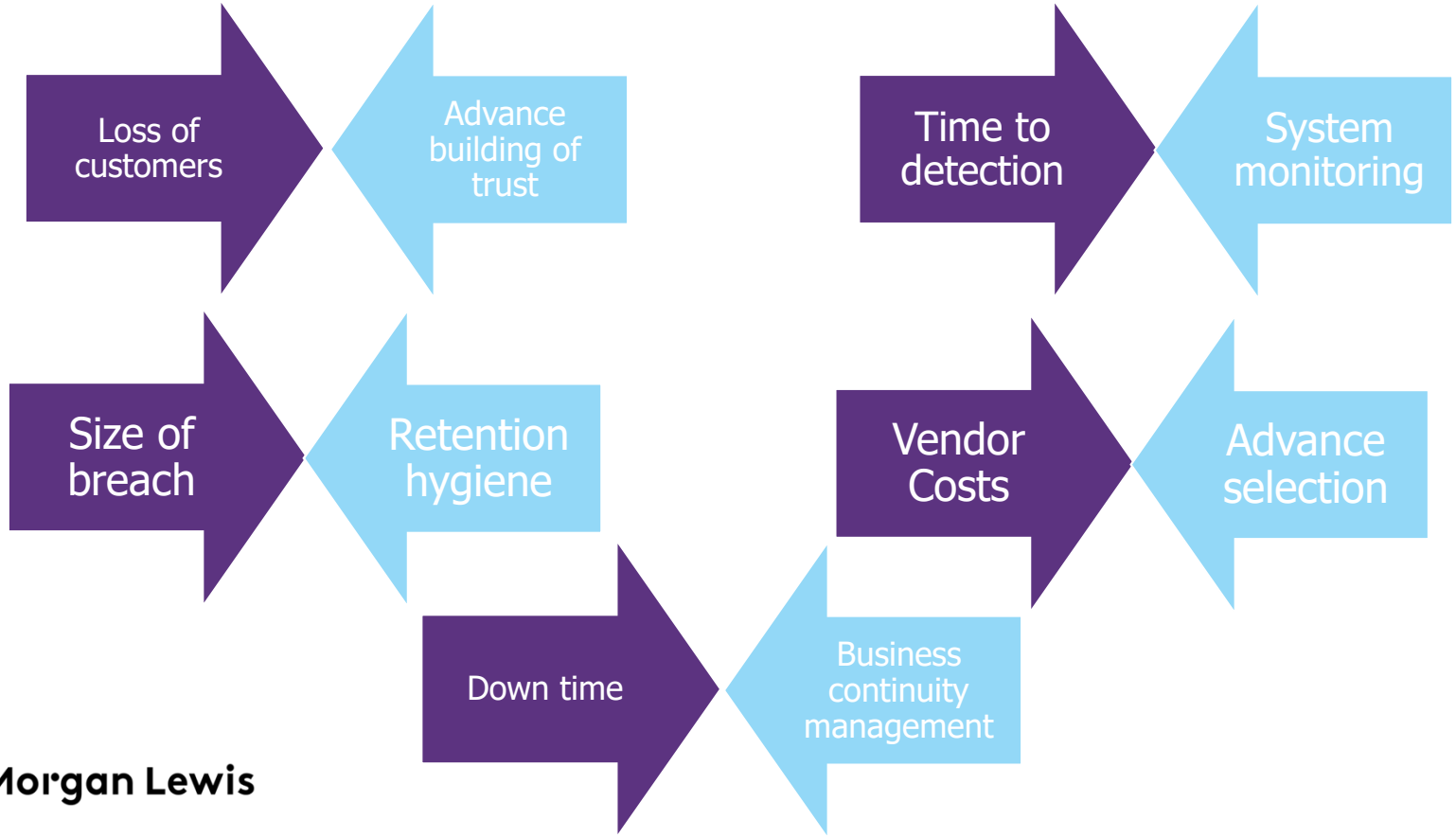
$16 per record

Why so much? Categories of costs:

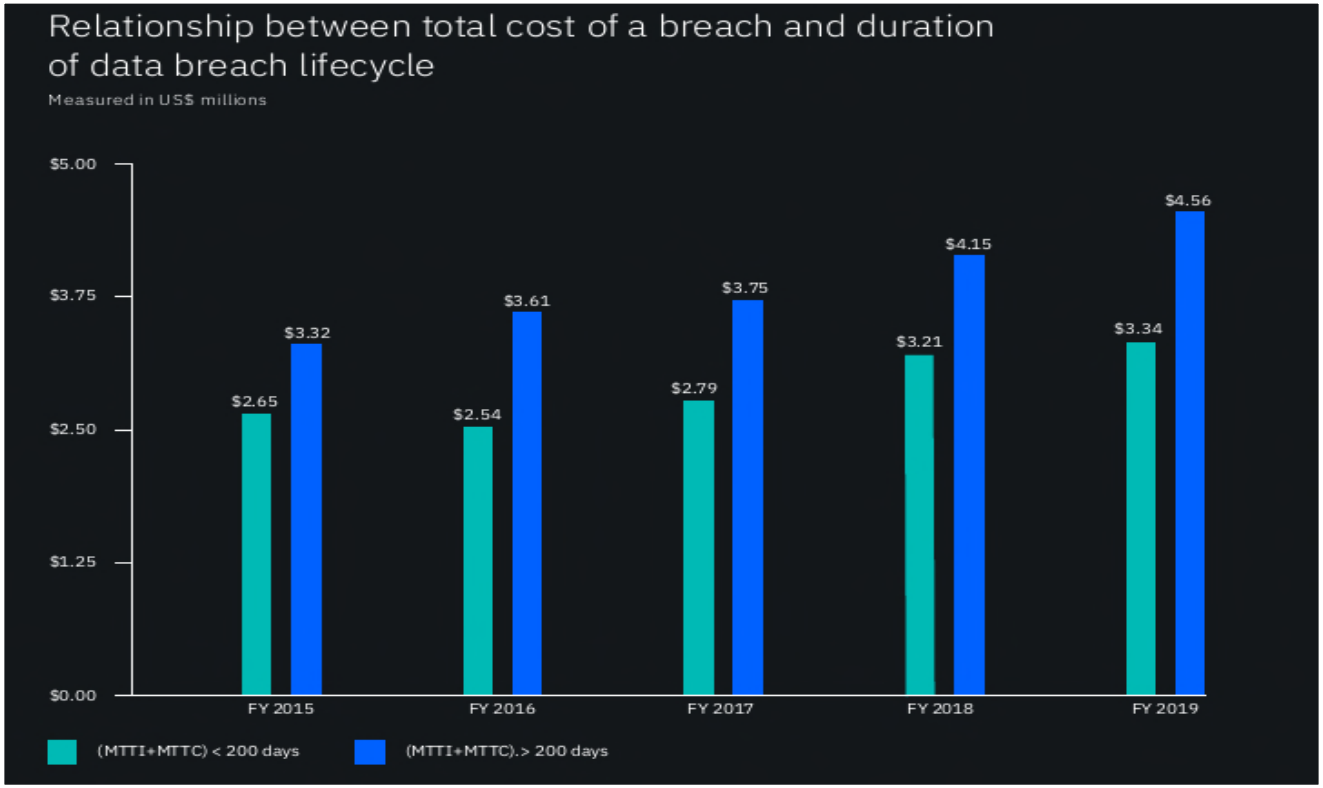
- Detection and escalation (forensics)
- Notification (letters, publicity)
- Lost business (downtime, customers)
- Aftermath (redress, litigation)

Source: Ponemon Cost of Data Breach Survey, 2019

Drivers of Data Breach Cost/Offsetting Controls

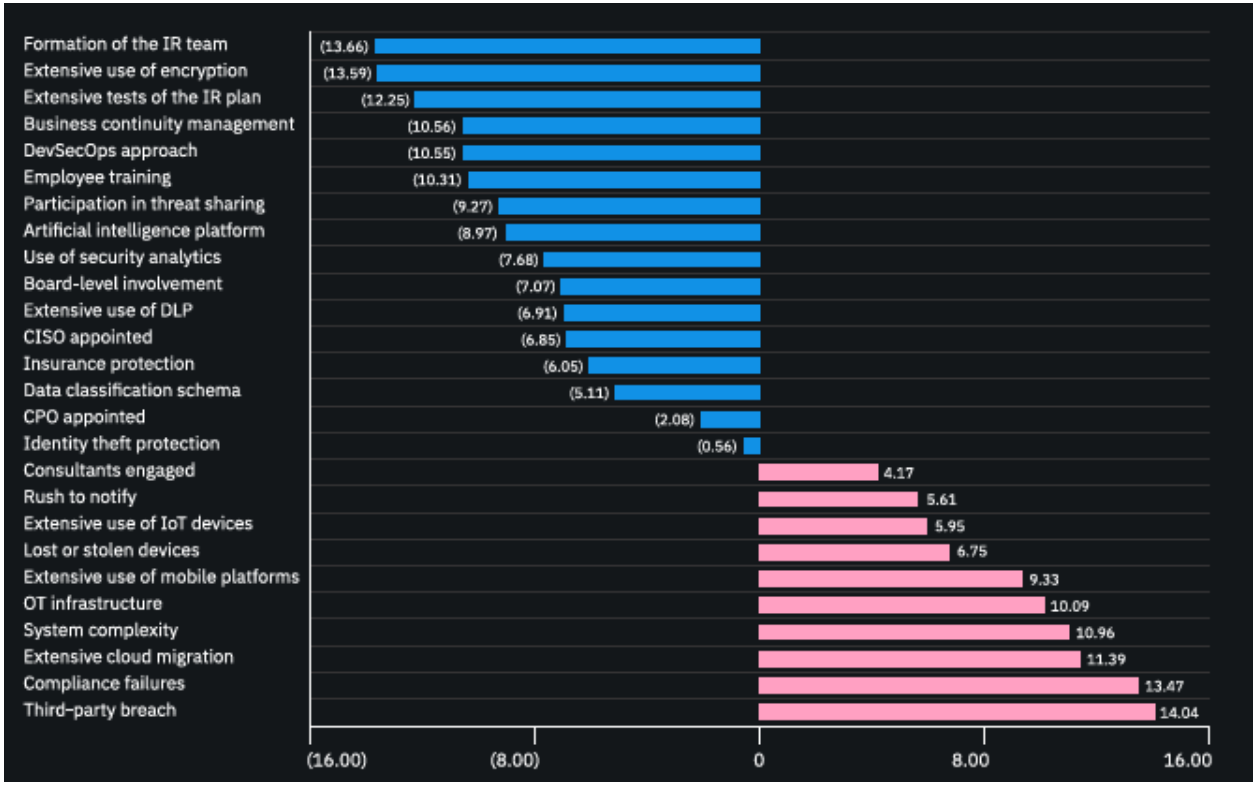


Identification and Containment = $2M+ Impact



Source: Ponemon Cost of Data Breach Survey, 2019

Factors That Decrease and Increase Breach Costs
(per record compromised, total average $150)



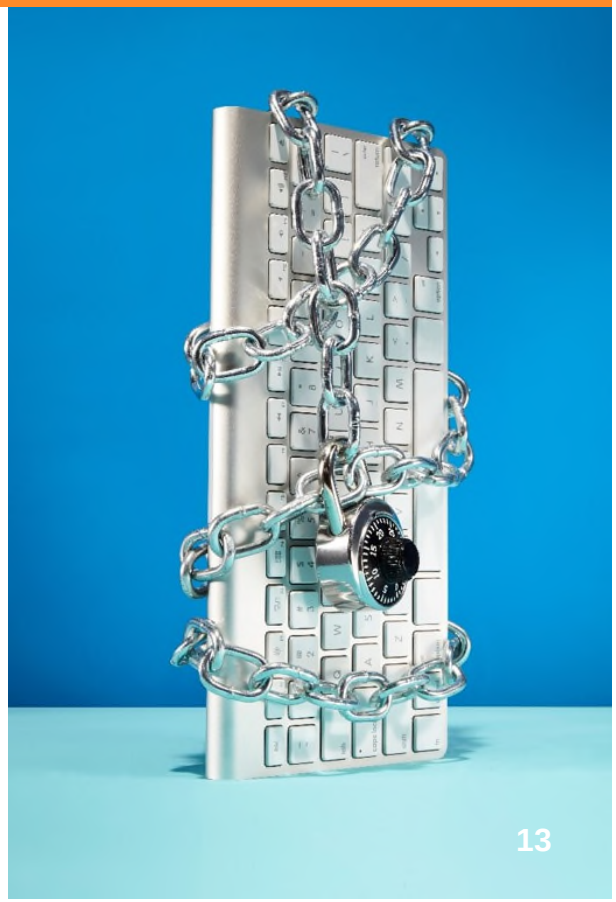
Source: Ponemon Cost of Data Breach Survey, 2019

SECTION 02

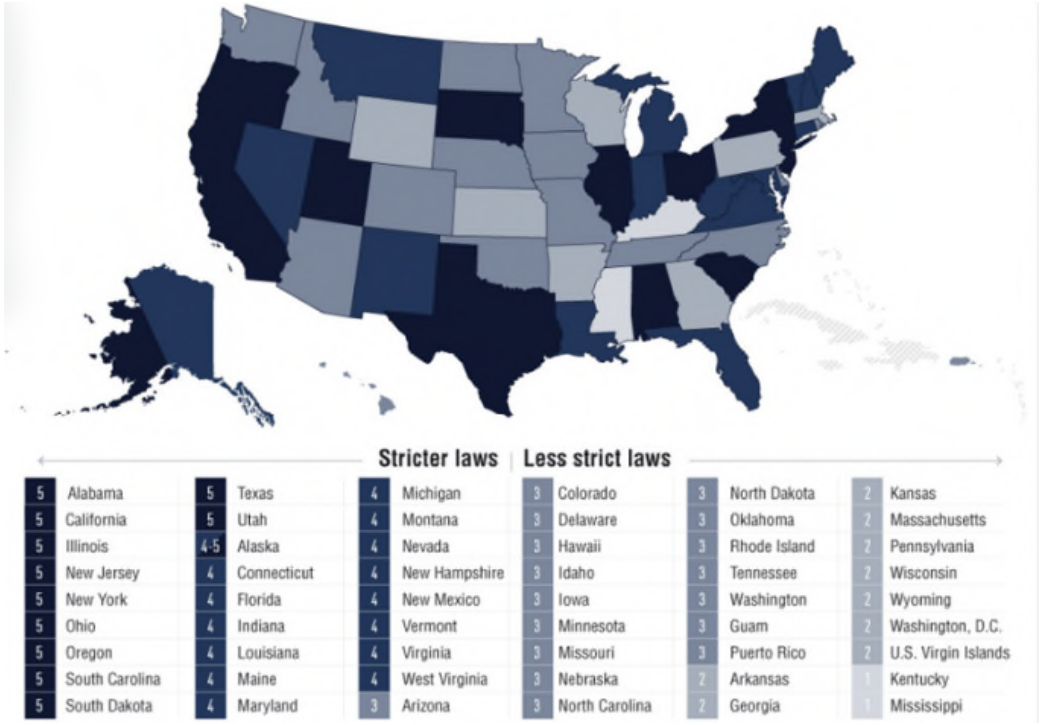
LEGAL LANDSCAPE

Legal Landscape

- State Data Breach Notification Laws
- EU GDPR Requirements
- DOJ Guidance
- FTC Guidance
- NIST Framework
- Negligence Standards
- Contractual Issues



State Data Breach Notification Laws – All 50+



Source: Digital Guardian, 2018

State Data Breach Notification Laws – The List

State	Citation
Alabama	2018 S.B. 318, Act No. 396
Alaska	Alaska Stat. § 45.48.010 *et seq.*
Arizona	Ariz. Rev. Stat. § 18-545
Arkansas	Ark. Code §§ 4-110-101 *et seq.*
California	Cal. Civ. Code §§ 1798.29, 1798.82
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. §§ 36a-701b, 4e-70
Delaware	Del. Code tit. 6, § 12B-101 *et seq.*
Florida	Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i)
Georgia	Ga. Code §§ 10-1-910, -911, -912; § 46-5-214
Hawaii	Haw. Rev. Stat. § 487N-1 *et seq.*
Idaho	Idaho Stat. §§ 28-51-104 to -107
Illinois	815 ILCS §§ 530/1 to 530/25
Indiana	Ind. Code §§ 4-1-11 *et seq.*, 24-4.9 *et seq.*
Iowa	Iowa Code §§ 715C.1, 715C.2
Kansas	Kan. Stat. § 50-7a01 et seq.
Kentucky	KRS § 365.732, KRS §§ 61.931 to 61.934
Louisiana	La. Rev. Stat. §§ 51:3071 *et seq.*
Maine	Me. Rev. Stat. tit. 10 § 1346 *et seq.*
Maryland	Md. Code Com. Law §§ 14-3501 *et seq.*, Md. State Govt. Code §§ 10-1301 to -1308
Massachusetts	Mass. Gen. Laws § 93H-1 *et seq.*
Michigan	Mich. Comp. Laws §§ 445.63, 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	Miss. Code § 75-24-29
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 *et seq.*, 33-19-321
Nebraska	Neb. Rev. Stat. §§ 87-801 *et seq.*
Nevada	Nev. Rev. Stat. §§ 603A.010 *et seq.*, 242.183
New Hampshire	N.H. Rev. Stat. §§ 359-C:19, 359-C:20, 359-C:21
New Jersey	N.J. Stat. § 56:8-161 *et seq.*
New Mexico	2017 H.B. 15, Chap. 36 (effective 6/16/2017)
New York	N.Y. Gen. Bus. Law § 899-AA, N.Y. State Tech. Law 208
North Carolina	N.C. Gen. Stat §§ 75-61, 75-65
North Dakota	N.D. Cent. Code §§ 51-30-01 *et seq.*
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. §§ 74-3113.1, 24-161 to -166
Oregon	Oregon Rev. Stat. §§ 646A.600 to .628
Pennsylvania	73 Pa. Stat. §§ 2301 *et seq.*
Rhode Island	R.I. Gen. Laws §§ 11-49.3-1 *et seq.*
South Carolina	S.C. Code § 39-1-90
South Dakota	S.D. Cod. Laws §§ 20-40-20 to -46 (2018 S.B. 62)
Tennessee	Tenn. Code §§ 47-18-2107; 8-4-119
Texas	Tex. Bus. & Com. Code §§ 521.002, 521.053
Utah	Utah Code §§ 13-44-101 *et seq.*
Vermont	Vt. Stat. tit. 9 §§ 2430, 2435
Virginia	Va. Code §§ 18.2-186.6, 32.1-127.1:05
Washington	Wash. Rev. Code §§ 19.255.010, 42.56.590
West Virginia	W.V. Code §§ 46A-2A-101 et seq.
Wisconsin	Wis. Stat. § 134.98
Wyoming	Wyo. Stat. §§ 40-12-501 *et seq.*
District of Columbia	D.C. Code §§ 28- 3851 *et seq.*
Guam	9 GCA §§ 48-10 et seq.
Puerto Rico	10 Laws of Puerto Rico §§ 4051 *et seq.*
Virgin Islands	V.I. Code tit. 14, §§ 2208, 2209

State Data Breach Notification Laws – The Basics

- Common elements:
  - Jurisdiction – doing business, residents
  - Compromise of security of information
  - Notification by mail or email to individuals
- Differ by state:
  - Triggering elements:
    - All states: SSN, DL#, financial account
    - Some states: Medical, password, biometrics
  - Exceptions for encryption or lack of harm
  - Notice content and level of detail
  - Notification to state authorities
  - Timing – "soon as practicable" to 30 days

GDPR – 72-Hour Notification Requirement

- Requires notification of Data Protection Authorities and individuals
- DPA Authority within 72 hours
  - Allows for "we do not know" submission
  - Follow up questions and reports
- Much broader set of triggering elements – any "personal information"
- BUT an exception for lack of harm
- Specifics vary by supervisory authority
- Other international laws – generally less strict

DOJ Guidance

Best Practices for Victim Response and Reporting of Cyber Incidents

Version 2.0 (September 2018)

- Educate senior management
- Identify your "crown jewels"
- Have an actionable plan in place . . . Now!
- Engage with law enforcement before an incident
- Procure services before an incident

FTC Guidance

DATA BREACH RESPONSE

A Guide for Business

- Team of experts:
  - Forensic
  - Legal
- Arrest the loss
- Preserve evidence
- Communications plan
- Notify as required
  - Individuals
  - Law enforcement/government
- Help protect "victims"

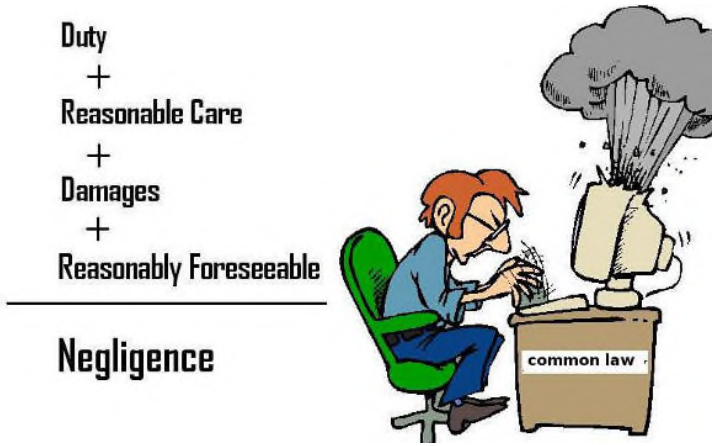
NIST Framework

NIST National Institute of Standards and Technology U.S. Department of Commerce

- **Detect** – must identify the occurrence of a cybersecurity event in a timely manner
- **Respond** – must take action regarding a detected cybersecurity incident to minimize impact
- **Recover** – must maintain plans for resilience and restore services impaired during cybersecurity incidents

Negligence Principles

- Still the most common cause of action in lawsuits and class actions
- Increasing standards on duty and reasonable care
- Inconsistent on damages and foreseeability
- "One free bite" rule



Contractual Issues

- Security standards
- Notification requirements
- Indemnity obligations
- Limitations of liability

SECTION 03

INCIDENT RESPONSE PLAN

Incident Response Plan -- Basics

- Best plans are teams and checklists
  - More like a brochure not a magazine or book
  - Team – internal and external:
    - Identify
    - Contact, backup contact
    - Roles
  - Checklists – questions, not what to do (~~playbook~~)
- Update annually
- Socialize and create awareness – particularly on triggering events

Morgan Lewis

DATA BREACH CHECKLIST

PHASE I:
ALERT AND ORGANIZATION

1. Company alerted to possible data breach—record date, time, and method of alert
2. Notify internal Incident Response Team (IRT), consisting of a representative from
    a. Information Technology
    b. Legal/Compliance
    c. Outside Counsel (Morgan Lewis)
    d. HR
    e. Public Relations
    f. Customer Service
    g. Executive
3. Identify an Incident Lead for this incident – performs as project manager
4. Contact outside counsel at Morgan Lewis
5. Convene conference call of IRT
6. Consider hiring forensic technology partner depending on available internal resources and complexity of breach
7. Notify insurance carrier/understand scope of preauthorization or limitations on third-party vendor reimbursement
8. Check with counsel on proper role and implementation of the attorney-client privilege in the data breach investigation

PHASE II:
INITIAL SCOPING BEFORE CONTAINING AN ONGOING BREACH

1. Identify, document, and preserve scope of compromise to the extent possible within 24–48 hours
2. Consider notifications or steps to take before stopping the breach that may prevent harm in the event the act of stopping the breach alerts data thieves that you have discovered them
3. Preserve any evidence related to the ongoing breach

PHASE III:
CONTAIN THE BREACH

1. Be sure that the full scope of compromise is understood to the extent possible within 24–48 hours
2. Contain/arrest the breach—stop any possible flow of data to unauthorized recipients
3. Document results of containment effort

PHASE IV:
INVESTIGATION

1. Root cause analysis
2. Classify type of breach
    a. Hacking
    b. Internal
    c. Loss/Theft of Tangible Data (computer, device, storage media)
    d. Inadvertent Disclosure
    e. Loss with No Known Disclosure
    f. Other
3. Full identification of data compromised
    a. Type of information compromised
        i. Sensitive personal information
            1. Social Security numbers
            2. Credit card information
            3. Financial account data
            4. Medical information
            5. Usernames and passwords
            6. Driver's license numbers
            7. Other sensitive personal information (disclosure of which could cause harm)
        ii. Other personal information
            1. Contact information (name, address, email address, phone number, etc.)
            2. Preferences, purchase history
            3. Other information linked to a person that is not sensitive
    b. Individuals whose information was compromised, including where they reside
4. Determine nature of any unauthorized recipients
    a. Employee acquisition in good faith
    b. Business partner
    c. Trustworthy recipient who normally receives information of this nature
    d. Unknown individuals, but definite disclosure
    e. Lost information—may not have been disclosed
    f. Suspected bad actor/employee not in good faith
    g. Known bad actor/departed or departing employee
5. Assess known or discoverable actual use of compromised information
6. Undertake security updates necessary before notification

PHASE V:
NOTIFICATIONS (IN LIGHT OF INFORMATION DEVELOPED IN PHASE IV)

1. Before notifications
    a. Develop PR plan for potential media inquiries
    b. Consider notification to company board of directors or others who should be notified before public
    c. Prepare for inquiries from affected individuals—call center or other
2. If criminal and depending on seriousness and other factors, notify law enforcement—local, FBI, Secret Service, or other
3. If required by law or recommended because individuals could do something to prevent further harm to themselves, make notifications to affected individuals. If made,
    a. Include what happened, what the company has done, and what the individual can do to prevent any harm
    b. Include legally required information and resources available from government agencies
    c. Consider an offer of identity theft prevention/credit monitoring depending on nature of information compromised
4. Notifications to government agencies and Attorneys General as required by law
5. Other notifications as required by information at issue
6. Evaluate feedback from notifications and determine if additional steps/notifications are required

PHASE VI:
POST-NOTIFICATIONS

1. Disclosures to investors, stockholders, SEC, securities disclosures, etc.
2. Cost recoveries—responsible third parties, insurance, other
3. Consider longer-term security upgrades or other measures to prevent reoccurrence or similar events
4. Analyze data breach notification plan/checklist for necessary changes in light of lessons learned
5. Prepare final reports
    a. Executive report with a summary of what happened, how it was addressed, what notifications were provided, and steps taken to prevent future incidents of the same or similar nature
    b. Technical report with detailed background of the event; evidentiary backup for analysis, decisions, and conclusions; and evidence of preventative measures

REMINDERS

- Maintain confidentiality—update IRT and executives frequently; other disclosures only to those who need to know
- Preserve evidence and information for future investigations
- Document events with dates and times; record reasons for determinations made
- The EU GDPR has a 72-hour deadline for some notifications; check early with outside counsel about whether it applies and how to manage it.

HOW WE CAN HELP

If we can be of assistance regarding your data collection, maintenance, protection, or suspected breach, contact a Morgan Lewis lawyer listed below:

Reece Hirsch | San Francisco
+1.415.442.1422 | reece.hirsch@morganlewis.com

Mark L. Krotoski | Silicon Valley
+1.650.843.7212 | mark.krotoski@morganlewis.com

Gregory T. Parks | Philadelphia
+1.215.963.5170 | gregory.parks@morganlewis.com

Pulina Whitaker | London
+44.20.3201.5550 | pulina.whitaker@morganlewis.com

Izzet Sinan | Brussels
+32.2.507.7522 | izzet.sinan@morganlewis.com

Charles Dauthier | Paris
+33.1.53.30.44.74 | charles.dauthier@morganlewis.com

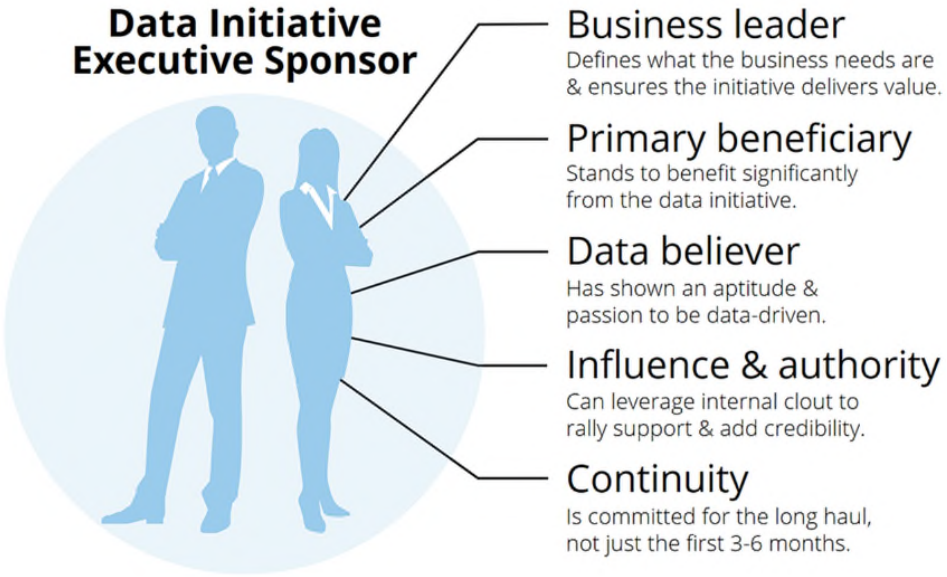
www.morganlewis.com

Incident Response Plan – Incident Response Team (IRT) – This Is a Team Sport!

- Executive Sponsor
- Incident Lead
- Information Technology
- Legal/Compliance
- Human Resources
- Public Relations
- Customer Service
- **As added or relieved by Incident Lead**
- Outside:
  - Legal
  - Forensic
  - Insurance
  - Credit monitoring

Roles -- Executive

- High-level sponsor
- Keeps C-Suite and Board apprised
- Makes material decisions
  - Shut down
  - Notification
  - Remediation
- Holds team members accountable
- Buck stops here
- Typically CIO, CISO, COO; sometimes CFO or CEO



Roles – Information Technology

- Coordinates input of information
- Pulls information for forensics
- Implements containment
- Remediates vulnerabilities
- Provides input to notification
- Typically serves Incident Lead role
- Must have broad view of IT, or have multiple IT representatives

Roles – Legal

- Advises on legal obligations
  - Notification
  - Preservation
  - Remediation
- Risk mitigation and management
  - Litigation
  - Regulatory
- Preserves privilege
- Engages outside counsel and vendors
- Typically a senior member of legal department with cybersecurity or litigation background

Roles – Public Relations

- Evaluates likelihood and content of public discourse
- Manages communications with press
- Drives public statements – press releases, social media, etc.
- Provides input on notification
- Coordinates with external PR firm
- Typically head PR or corporate communications person

Roles – Human Resources

- Provides input where employee data is involved in incident
- Considers and provides feedback on communications to employees
- Determines appropriate training for incident and post-incident response
- Typically a senior member of HR team with knowledge of HR data practices

Roles – Finance

- Evaluates potential impact of event on company's financial performance and systems
- Contributes to decisions on financial reporting of incident
- Accrues appropriate reserves for incident and aftermath
- Typically a senior member of finance or accounting team

Roles – Customer Service

- Anticipates increased customer questions and plans to decrease customer churn post-incident
- Coordinates with credit monitoring call site
- Determines and helps mitigate likely long-term effect on customer base
- Typically a senior member of customer service department

Logistics of Response

- A good plan anticipates how to connect members of the IRT in all circumstances
- Incidents never occur at convenient times
- Expansive contact information
- Backups
- Reverse-911
- Practicing – mocks or little incidents

Privilege

- Communications necessary to allow counsel to render legal advice
- Differs with
  - Outside counsel
  - Forensic investigator
  - Public relations consultant
- Having lawyer involved increases but does not guarantee protection
- Flexibility important

Preservation and Communication Security

- Preserve those artifacts, documents, and data that will be important
- Balancing restoration versus preservation
- Need-to-know basis
- Communication security on impaired platforms
- Recognize costs and trade-offs

Be An Active Incident Response Team!

- Meet on a regular basis (monthly, every other month, quarterly depending)
- Update all contact information
- Review latest developments:
  - Internally on data security
  - Attacks that were not a compromise
  - Externally – public events

SECTION 04

OUTSIDE EXPERTS

Outside Experts

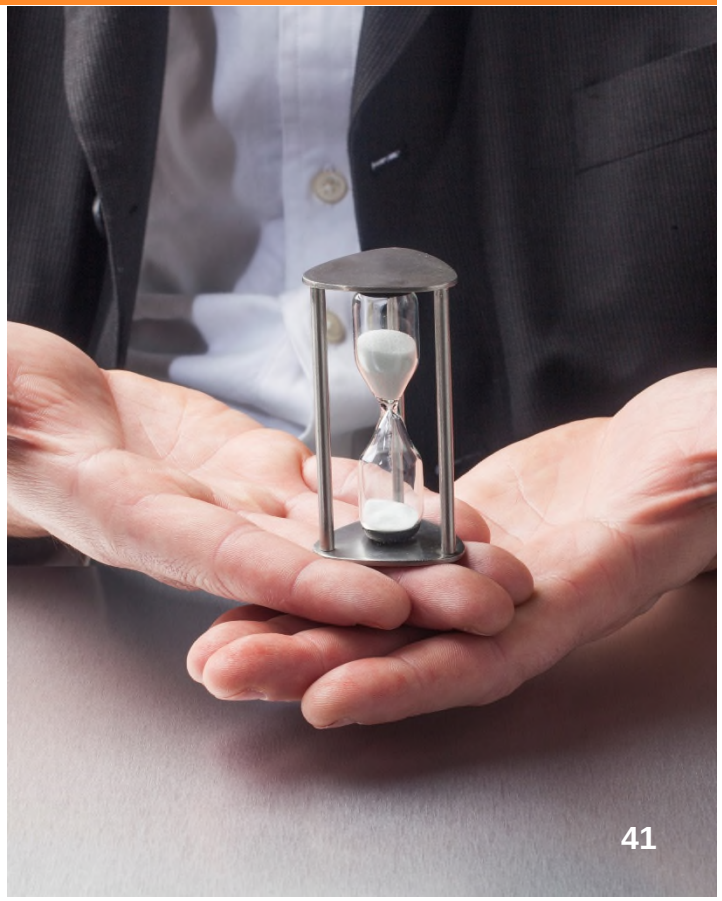
- Forensic
- Legal
- Credit Monitoring and Mail House
- Credit
- Insurance

SECTION 05

THE RESPONSE

First 72 Hours

- Identify and document source of initial information
- Preserve
- Contain
- Gather necessary internal and external team
- Notify insurance carrier
- Determine scope
- Identify information to gather
- Classify type and severity of incident – drives "who is calling the shots?"
- Notify executives/the board
- GDPR 72 hour notification if required



The Long Middle

- Investigate
  - Root causes
  - Scope and impact:
    - Elements
    - Individuals
    - Residence/Geography
  - Potential harm
- Notify – individuals, government, law enforcement, business partners, others?
- Remediate

The "End"

- Determine financial disclosures
- Feedback:
  - IRT membership and performance
  - Incident Response Plan revisions
- Cost recoveries
- Final reports:
  - Technical – background, facts, evidence, preserved media
  - Executive – what happened, decisions and rationales, notifications, steps taken to prevent reoccurrence
- Calendar 6-month follow-up

Questions?

Gregory T. Parks

Gregory T. Parks
Philadelphia
+1.215.963.5170
gregory.parks@morganlewis.com

Greg Parks is the co-leader of the firm's privacy and cybersecurity practice and retail & eCommerce industry sector. Greg counsels and defends retail companies and other consumer facing clients in matters related to privacy and cybersecurity, class actions and Attorney General actions, consumer protection laws, loyalty and gift card programs, retail operations, payment mechanisms, product liability, waste management, shoplifting prevention, compliance, antitrust, and commercial disputes. In the aftermath of data breaches—he's advised on more than 800 breaches in his career—Greg helps clients craft immediate responses. He counsels them on how best to give notice to affected individuals or government and consumer reporting entities, following proper compliance protocol. He also represents these companies on any data class action and other litigation stemming from the incidents, and instructs them on implementing policies and procedures to prevent and mitigate future breaches.

Ezra D. Church

Parks Ezra D. Church
Philadelphia
+1.215.963.5710
ezra.church@morganlewis.com

Ezra D. Church focuses his practice on class action lawsuits and complex commercial and product-related litigation, with particular emphasis on the unique issues facing retail, ecommerce, and other consumer-facing companies. Ezra also focuses on privacy and data security matters, and regularly advises and represents clients in connection with these issues. He is co-chair of Morgan Lewis's Class Action Working Group.

Ezra has extensive experience handling complex and unusual class action litigation, and has handled all aspects of such cases from inception through trial and appeal. His work in this area includes defeat of class certification in a rare copyright class action against one of the world's leading publishers, successful opposition of class certification in an unusual defendant class action against many large financial institutions, and a successful defense verdict in a consumer class action trial against an international retailer, including affirmance on appeal. He is an active member of the Firm's Class Action Working Group and regularly writes and speaks on class action issues. He is a contributor to the Firm's chapter on class action litigation in the leading treatise Business and Commercial Litigation in Federal Courts and co-author of a chapter in A Practitioner's Guide to Class Actions, among others.

Kristin M. Hadgis

Kristin M. Hadgis
Philadelphia
+1.215.963.5563
kristin.hadgis@morganlewis.com

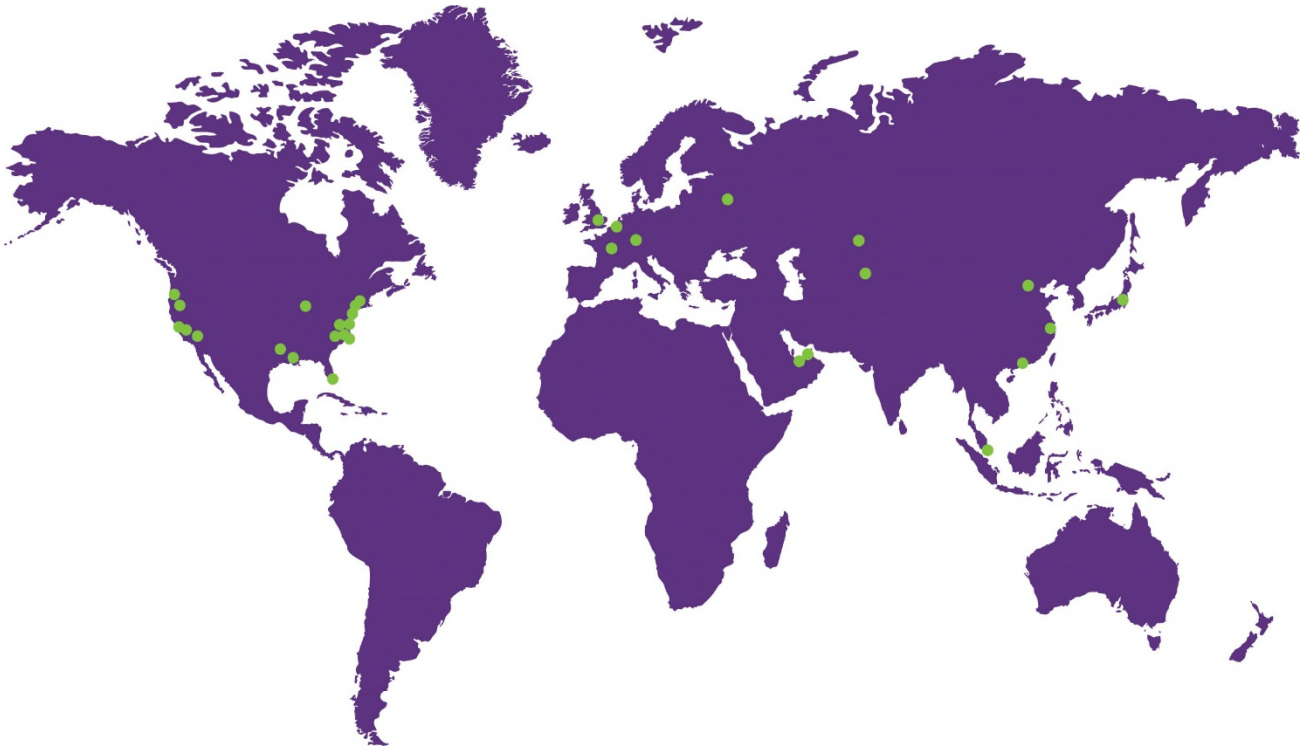
Kristin has represented companies faced with class actions and government investigations, and has advised hundreds of companies in connection with data breaches and privacy and cybersecurity compliance issues such as privacy policies, information security policies, incident response plans, and protocols for data collection, storage, and transfer. Her experience includes the General Data Protection Regulation (GDPR), state data security laws, the Fair Credit Reporting Act (FCRA), the Fair and Accurate Credit Transactions Act (FACTA), US federal and state CAN-SPAM laws, the Telephone Consumer Protection Act (TCPA), Federal Trade Commission (FTC) rules, the Securities and Exchange Commission privacy regulations (Reg. S-P), the Children's Online Privacy Protection Act (COPPA), and the Family Educational Rights and Privacy Act (FERPA).

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU